

Aktywacja certyfikatu Certum S/MIME Mailbox

Wer. 1.1

assecO

 **Certum**
by assecO

Spis treści

1. Opis produktu	3
2. Aktywacja certyfikatu	3
Krok Weryfikacja e-mail	3
Metoda CSR	6
Metoda generowania kluczy na karcie kryptograficznej	6
Podanie adresu e-mail.....	9
Krok Aktywacja certyfikatu	10

1. Opis produktu

Zabezpiecz swoją pocztę e-mail, dzięki podpisywaniu i szyfrowaniu komunikacji z użyciem certyfikatów Certum S/MIME.

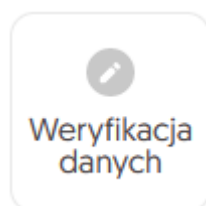
Dzięki unikalnej funkcji podpisu i szyfrowania zyskasz pewność, że wysyłane przez Ciebie e-maile są odpowiednio zabezpieczone przed ich potencjalnym wyciekiem lub modyfikacją oraz zapewnisz odbiorcę o swojej tożsamości.

Certyfikat Certum S/MIME ma wszechstronne zastosowanie. Możesz go również użyć do zabezpieczenia swojej stacji Windows, wykorzystując funkcję uwierzytelnienia użytkownika w systemach lub aplikacjach.

2. Aktywacja certyfikatu

Rozpoczęcie procesu aktywacji będzie możliwe z poziomu **Twojego konta** w sklepie, w zakładce **Produkty bezpieczeństwa**. Proces składa się z kilku kroków:

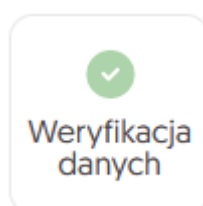
- **Weryfikacja e-mail** – wygenerowanie kluczy i podanie e-mail oraz jego weryfikacja
- **Aktywacja certyfikatu** – wybór pól do certyfikatu i przekazanie go do wydania.



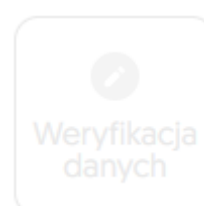
Krok oczekuje na podanie danych



Podano dane, dane oczekują na zakończenie weryfikacji



Dane zostały zweryfikowane



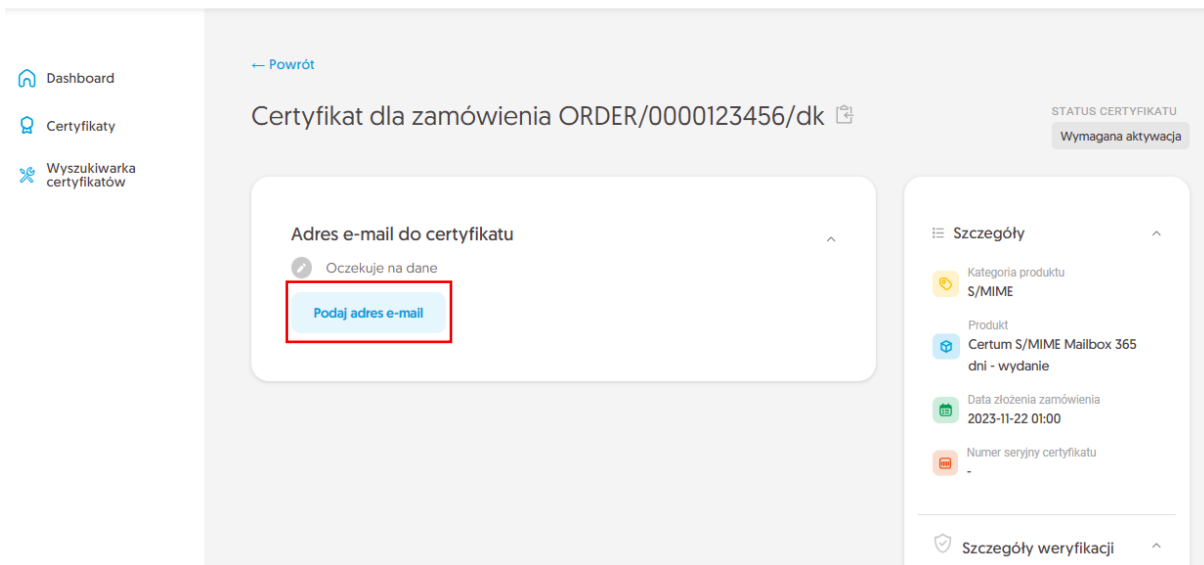
Podanie danych jest jeszcze niedostępne

Krok Weryfikacja e-mail

Rozpoczęcie generacji pary kluczy i podania e-mail możesz poprzez **Dashboard**, wybierając opcję **Weryfikacja e-mail**:

The screenshot shows the Certum dashboard interface. On the left is a sidebar with navigation links: Dashboard, Certyfikaty, and Wyszukiwarka certyfikatów. The main content area is divided into several sections. At the top left, a 'Cześć' (Hello) message welcomes the user. Below it is an 'Aktualności' (News) section with a placeholder for a box icon and the text 'Brak aktualności do wyświetlenia.' (No news to display). To the right of the welcome message is a 'Przydatne informacje' (Useful information) section with a description of the activation process and a 'Przydatne linki' (Useful links) section with links to automatic subscriber verification, help documents, CSR/PFX generator, and products. The bottom section is titled 'S/MIME' and shows the order number 'ORDER/0000123456/dk'. It contains two buttons: 'Weryfikacja e-mail' (highlighted with a red box) and 'Aktywacja certyfikatu'. Below these buttons, the product details are listed: 'Produkt: Certum S/MIME Mailbox 365 dni - wydanie', 'Status: Wymagana aktywacja', 'Common name: -', and 'Data końca ważności certyfikatu: -'. A link 'Szczegóły certyfikatu' is at the bottom.

lub z listy **Certyfikaty** – wybierz certyfikat, który chcesz aktywować i w szczegółach wybierz opcję **Podaj adres e-mail**.

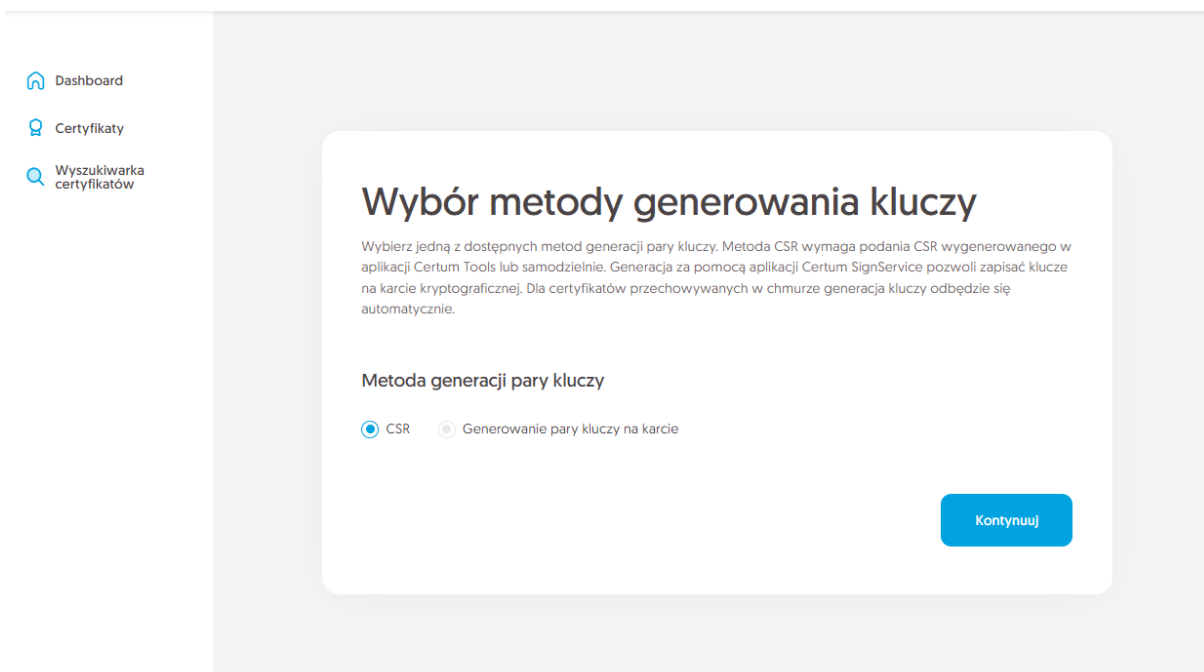


W tym kroku wygenerujesz parę kluczy oraz podasz adres e-mail do umieszczenia w certyfikacie.

Dla certyfikatów S/MIME dostępnymi metodami generacji kluczy są:

- **CSR** – żądanie podpisania certyfikatu, wygenerowane poprzez generator np. [Certum Tools](#) lub aplikację/serwer, na którym będzie zainstalowany certyfikat
- **Generowanie pary kluczy na karcie** – klucze zostaną zapisane na karcie kryptograficznej.

Wybierając metodę generowania pary kluczy na karcie, wybierz również algorytm i długość klucza. Twój wybór powinien zależeć od algorytmu i długości klucza wspieranej przez aplikację, w której używasz certyfikatu lub rekomendację np. Twojego działu IT.



Metoda CSR

Po wybraniu metody CSR, możesz przejść dalej do podania CSR. Na tym etapie będziesz mógł pobrać aplikację [Certum Tools](#) do wygenerowania CSR lub dostarczyć własny.

Po przejściu dalej, wklej posiadany CSR. Po wklejeniu CSR, zostanie on zweryfikowany czy jest poprawny. W razie wystąpienia błędu CSR, pojawi się o tym informacja w komunikacie błędu.



Pamiętaj, aby w przypadku wygenerowania CSR w generatorze, zapisać i zachować klucz prywatny. Będzie on niezbędny do zainstalowania certyfikatu po jego wydaniu.

Podanie prawidłowego CSR i przejście dalej pozwoli podać e-mail do certyfikatu.

Metoda generowania kluczy na karcie kryptograficznej

Po wybraniu metody generowania pary kluczy na karcie, wybierz algorytm i długość klucza.

Wybór metody generowania kluczy

Wybierz jedną z dostępnych metod generacji pary kluczy. Metoda CSR wymaga podania CSR wygenerowanego w aplikacji Certum Tools lub samodzielnie. Generacja za pomocą aplikacji Certum SignService pozwoli zapisać klucze na karcie kryptograficznej. Dla certyfikatów przechowywanych w chmurze generacja kluczy odbędzie się automatycznie.

Metoda generacji pary kluczy

☐ CSR ☒ Generowanie pary kluczy na karcie

ALGORYTM KLUCZA I DŁUGOŚĆ KLUCZA

Wybierz algorytm i długość klucza ▼




Metoda CSR pozwoli uzyskać certyfikat wraz z kluczem w formie do przenoszenia i instalacji z pliku. Pamiętaj, by zapisać klucz prywatny, który wygenerowałeś wraz z CSR.

i Wygenerowanie kluczy na karcie spowoduje, że wydany certyfikat zostanie zainstalowany na karcie kryptograficznej i jej podłączenie do komputera będzie wymagane zawsze, gdy certyfikat jest używany. Wspierane są tylko karty Certum.

Kontynuuj

Po przejściu dalej, upewnij się, że posiadasz kartę włożoną do czytnika, czytnik podłączony do komputera, a sama karta ma zainicjalizowany profil zwykły z nadanym kodem PIN. W procesie wymagane jest również posiadanie zainstalowanej na komputerze aplikacji proCertum CardManager, w której możesz również sprawdzić status karty i kodów PIN i PUK.

Zapraszamy do zapoznania się z instrukcją [jak nadać kod PUK i PIN dla profilu zwykłego karty](#).

-  Dashboard
-  Certyfikaty
-  Wyszukiwarka certyfikatów


- 1 Generacja kluczy
- Podanie e-maila
- Podsumowanie

Generacja kluczy

W celu wygenerowania kluczy, zastosuj instrukcję dostępną poniżej.

 [Pobierz aplikację Certum SignService](#)

1. Pobierz i zainstaluj aplikację **Certum SignService**.
2. Pobierz i zainstaluj aplikację **proCertum CardManager**, jeśli jej nie posiadasz lub jest nieaktualna.
3. Podłącz czytnik do komputera i włóż kartę do czytnika.
4. Otwórz aplikację **proCertum CardManager** i sprawdź czy profil zwykły karty jest zainicjalizowany.
Jeśli profil nie jest zainicjalizowany, aplikacja poprosi Cię o nadanie kodów PIN i PUK.
5. Rozpocznij generację kluczy przyciskiem **Wygeneruj klucze**.
6. Zaakceptuj komunikat z przeglądarki o zgodę na uruchomienie aplikacji Certum SignService.
7. Gdy pojawi się okno aplikacji Certum SignService, wprowadź PIN do profilu zwykłego karty.
8. Oczekaj na wygenerowanie kluczy, może to zająć do kilku minut.

 Po zakończeniu generacji, zostaniesz przeniesiony do kolejnego okna procesu.

[Cofnij](#)




Wygeneruj klucze

Do wygenerowania kluczy na karcie potrzebujesz również zainstalowaną na komputerze aplikację Certum SignService. Aplikacja Certum SignService po uruchomieniu generowania kluczy, poprosi o zgodę na uruchomienie się i podanie kodu PIN profilu zwykłego karty w celu wygenerowania na niej kluczy.

http://100.101.10.90:4300 chce otworzyć tę aplikację.

Otwórz CertumSignService

Anuluj

-  Dashboard
-  Certyfikaty
-  Wyszukiwarka certyfikatów

- 1 Generacja kluczy
- Podanie e-maila
- Podsumowanie



The image shows a software window titled "Certum SignService" with a close button (X) in the top right corner. Inside the window, there is a logo consisting of a blue icon of a computer monitor with a quill pen writing on it, followed by the text "Certum SignService" in a large, bold, black font, and "by GISECO" in a smaller blue font below it. Below the logo, the heading "Generacja nowej pary kluczy" (Generation of a new key pair) is displayed in bold. There are two sections: "Dane karty" (Card data) and "Dane klucza" (Key data). The "Dane karty" section contains two fields: "Nazwa czytnika:" (Reader name) with the value "ACS ACR39U ICC Reader 0" and "Numer karty:" (Card number) with the value "2268 9624 6429 8967". The "Dane klucza" section contains two fields: "Algorytm:" (Algorithm) with the value "RSA" and "Wielkość:" (Size) with the value "2048". Below these sections, there is a label "PIN profilu zwykłego:" (Regular profile PIN:) followed by a text input field. Below the input field, the text "[od 4 do 8 znaków]" (from 4 to 8 characters) is displayed. Further down, there are two lines of bold text: "W zależności od algorytmu i wielkości klucza generacja może potrwać do kilku minut" (Depending on the algorithm and key size, generation may take up to several minutes) and "W trakcie operacji nie wyjmuj karty z czytnika" (During the operation, do not remove the card from the reader). At the bottom right, there are two buttons: "Ok" and "Anuluj" (Cancel).

Dane karty	
Nazwa czytnika:	ACS ACR39U ICC Reader 0
Numer karty:	2268 9624 6429 8967

Dane klucza	
Algorytm:	RSA
Wielkość:	2048

PIN profilu zwykłego:

[od 4 do 8 znaków]




W zależności od algorytmu i wielkości klucza generacja może potrwać do kilku minut

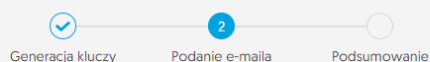
W trakcie operacji nie wyjmuj karty z czytnika

Po wpisaniu kodu PIN rozpocznie się proces generowania klucza na karcie. Może to zająć do kilkudziesięciu sekund. Wygenerowanie klucza pozwoli podać e-mail do certyfikatu.

Podanie adresu e-mail

Wprowadź adres e-mail i przejdź do podsumowania.

-  Dashboard
-  Certyfikaty
-  Wyszukiwarka certyfikatów



Wprowadź e-mail

Wprowadź adres e-mail, który chcesz umieścić w certyfikacie. Adres będzie wymagał weryfikacji dostępu do niego.

ADRES E-MAIL*

Wprowadź adres e-mail

Kontynuuj

Zweryfikuj wprowadzone dane na ekranie podsumowania. Jeśli dane są poprawne, zakończ krok podawania adresu e-mail.

Ekran sukcesu poinformuje Cię o zapisaniu adresu e-mail. Przeprowadź jego weryfikację. Po ukończeniu weryfikacji adresu e-mail jego status powinien zmienić się na „zweryfikowano”, co pozwoli przejść do ostatniego kroku, czyli **Aktywacji certyfikatu**.

Krok Aktywacja certyfikatu

Aktywację certyfikatu możesz rozpocząć poprzez **Dashboard**, wybierając opcję **Aktywacja certyfikatu** lub analogicznie jak w poprzednim kroku: z listy **Certyfikaty** – wybierz certyfikat, który chcesz aktywować i w szczegółach wybierz opcję **Aktywuj certyfikat**.

Dashboard

Certyfikaty

Wyszukiwarka certyfikatów

Wybór danych do certyfikatu Podsumowanie

Wybór danych do certyfikatu

Wybierz dane i parametry, które będą widoczne w certyfikacie. Niektóre z pól są wymagane w danym produkcie i nie ma możliwości ich odznaczenia.

S/MIME
Certum S/MIME Mailbox 365 dni - wydanie

Adres e-mail [E]:
jankowalski@twojadenomena.pl

Common name:
jankowalski@twojadenomena.pl

Przejdź na ekran podsumowania i sprawdź wszystkie dane. Oznacz wymagane oświadczenia i zakończ aktywację certyfikatu.

Ekran sukcesu poinformuje Cię o przekazaniu certyfikatu do wydania. Wydany certyfikat można będzie pobrać z wiadomości e-mail o utworzeniu certyfikatu lub z widoku szczegółów certyfikatu: w dogodnym kodowaniu **PEM** lub **DER** lub zainstalować na karcie, również z poziomu szczegółów certyfikatu.

W widoku szczegółów certyfikatu możesz również pobrać certyfikaty pośrednie dla Twojego certyfikatu.

Jeśli potrzebujesz pliku PFX, możesz skorzystać z generatora [Certum Tools](#).